UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of A pink/peach Samsung cellular phone with IMEI 351488824003851, seized on August 2, 2022, as described more fully in Attachment A.	))))))	Case No. **2:22-MJ-03737**

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☒ evidence of a crime;

☒ contraband, fruits of crime, or other items illegally possessed;

☒ property designed for use, intended for use, or used in committing a crime;

☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 2252A(a)(2), 2252A(a)(5)(B)	Receipt and Distribution of Child Pornography; Access With Intent to View and Possession of Child Pornography

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

/s/ Sean D. Lusk

Applicant's signature

Sean Lusk, FBI Task Force Officer

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: _____

Judge's signature

City and state: Los Angeles, CA

Alexander F. MacKinnon, U.S. Magistrate Judge

Printed name and title

AUSA: Kathrynne Seiden (x0631)

ATTACHMENT A

PROPERTY TO BE SEARCHED

A pink/peach Samsung cellular phone with IMEI # 351488824003851, seized on August 2, 2022, and currently in the custody of the FBI in Santa Barbara County (the "SUBJECT DEVICE").

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2) (receipt and distribution of child pornography) and 2252A(a)(5)(B) (access with intent to view and possession of child pornography) (collectively, the "Subject Offenses"), namely:

a. Child pornography, as defined in 18 U.S.C. § 2256(8).

b. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that refer to child pornography, as defined in 18 U.S.C. § 2256(8), including but not limited to, documents that refer to the possession, receipt, distribution, transmission, reproduction, viewing, sharing, purchase, or downloading, production, shipment, order, requesting, trade, or transaction of any kind, involving child pornography.

c. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, tending to identify persons involved in the possession, receipt, distribution, transmission, reproduction, viewing, sharing, purchase, or downloading, production, shipment, order, requesting, trade, or transaction of any kind, involving child pornography, as defined in 18 U.S.C. § 2256(8).

d. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages,

that identify any minor visually depicted while engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2)(B).

e. Any records, documents, programs, applications, or materials or items which are sexually arousing to individuals who are interested in minors, but which are not in and of themselves obscene or which do not necessarily depict minors involved in sexually explicit conduct. Such material is commonly known as "child erotica" and includes written materials dealing with child development, sex education, child pornography, sexual abuse of children, incest, child prostitution, missing children, investigative techniques of child exploitation, sexual disorders, pedophilia, nudist publications, diaries, and fantasy writings.

f. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that pertain to peer-to-peer file-sharing software.

g. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that pertain to accounts with any Internet Service Provider.

h. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, regarding ownership and/or possession of the SUBJECT DEVICE.

i. With respect to the SUBJECT DEVICE used to facilitate the above-listed violations or containing evidence falling within the scope of the foregoing categories of items to be seized:

j. evidence of who used, owned, or controlled the SUBJECT DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

k. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

l. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the SUBJECT DEVICE;

m. evidence of the times the SUBJECT DEVICE was used;

n. passwords, encryption keys, and other access devices that may be necessary to access the SUBJECT DEVICE;

o. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the SUBJECT DEVICE or to conduct a forensic examination of it;

p. records of or information about Internet Protocol addresses used by the SUBJECT DEVICE.

SEARCH PROCEDURES FOR THE SUBJECT DEVICE

2. In searching the SUBJECT DEVICE (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") may search the SUBJECT DEVICE.

b. The search team will, in its discretion, either search the SUBJECT DEVICE where it is currently located or transport it to an appropriate law enforcement laboratory or similar facility to be searched at that location.

c. The search team shall complete the search of the SUBJECT DEVICE as soon as is practicable but not to exceed 120 days from the date of issuance of the warrant. The government will not search the digital device beyond this 120-day period without obtaining an extension of time order from the Court.

d. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in the SUBJECT DEVICE to the search protocols to determine whether the SUBJECT DEVICE and any data therein falls within the scope of the items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of the items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques, including to search for known images of child pornography.

e. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

f. If the search determines that the SUBJECT DEVICE does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the SUBJECT DEVICE and delete or destroy all forensic copies thereof.

g. If the search determines that the SUBJECT DEVICE does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

h. If the search determines that the SUBJECT DEVICE is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside

the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

i. The government may also retain the SUBJECT DEVICE if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

j. After the completion of the search of the SUBJECT DEVICE, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

3. This warrant authorizes a review of electronic storage media seized, electronically stored information, communications, other records and information seized, copied or disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

4. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

Affidavit

I, Sean D. Lusk, being duly sworn, declare and state as follows:

I. AFFIANT'S BACKGROUND

1. I am a Task Force Officer ("TFO") with the FBI assigned to the Central Coast Safe Streets Task Force. I am also employed as a full-time, sworn law enforcement officer for the California Highway Patrol ("CHP") and have been so employed for the past 23 years. I am currently assigned to the Coastal Division Investigative Services Unit. My primary responsibility is to investigate and assist other officers and allied agencies with in-depth investigations involving criminal street gangs, weapons, and narcotics violations.

2. I attended and graduated from the California Highway Patrol Academy and hold Basic, Intermediate, and Advanced Certificates from California Peace Officer Standards and Training. I have completed a 72-hour Drug Recognition Expert course certified by the International Association of Chiefs of Police and over 80 hours of narcotics and criminal interdictions training relating to the transportation, concealment, trends, and sales of illegal narcotics and other criminal activities. I have spoken on numerous occasions with other officers and experts in the field of narcotics interdiction regarding current trends on narcotic sales and trafficking.

3. As a TFO, I have participated in numerous investigations involving federal firearm and drug offenses and

participated in the execution of numerous arrest and search warrants. I have also participated in the interviews of defendants, informants, and witnesses who had personal knowledge of firearm and drug trafficking methods and have conducted or assisted in the review of numerous digital devices.

II. PURPOSE OF AFFIDAVIT

4. I make this affidavit in support of an application for a warrant to search the digital device described in Attachment A (the "SUBJECT DEVICE"), specifically, a pink/peach Samsung cellular phone with IMEI 351488824003851, seized on August 2, 2022, and currently in the custody of the FBI in Santa Barbara County.

5. As discussed below, I respectfully submit there is probable cause to believe that evidence, fruits, instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2) (receipt and distribution of child pornography) and 2252A(a)(5)(B) (access with intent to view and possession of child pornography) (the "Subject Offenses"), as described further in Attachment B, will be found within the SUBJECT DEVICE. Attachments A and B are incorporated herein by reference.

6. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from other law enforcement personnel and

witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only and all dates are approximate.

III. STATEMENT OF PROBABLE CAUSE

7. On August 11, 2022, the Honorable Alexander F. MacKinnon, United States Magistrate Judge for the Central District of California, authorized a search warrant for two digital devices, including the SUBJECT DEVICE, in Case Number 2:22-MJ-03149. The application submitted in support of that search warrant is incorporated herein by reference and attached hereto as **Exhibit 1**.

8. On August 12, 2022, pursuant to the warrant, I began to review the contents of the SUBJECT DEVICE. On August 13, 2022, at approximately 3:15 PM, I saw an image depicting what appeared to be child pornography. Upon recognizing the image as possible child pornography, I discontinued review of the SUBJECT DEVICE.

9. On August 15, 2022, I consulted with FBI Special Agent Ashley Gaines, who investigates crimes against children involving the Internet and computers. Special Agent Gaines and I opened a forensic copy of the SUBJECT DEVICE to retrieve the image I saw on August 13, 2022. I was not able to locate the

initial image I had seen. However, while looking for the image, SA Gaines and I saw a second image on the SUBJECT DEVICE. SA Gaines related to me that based upon her training and experience, this second image appeared to depict a female, approximately 12 years old, being penetrated by an adult male.

IV. TRAINING & EXPERIENCE ON INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN

10. Based on my training and experience, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who view and possess multiple images of child pornography are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or in other visual media, or from literature describing such activity. These individuals often maintain possession of these items for long periods of time and keep their collections in numerous places – in digital devices in their homes, in their cars, in their workplaces, or on their persons.

b. Individuals who have a sexual interest in children or images of children also may correspond with and/or

meet others to share information and materials (including through digital distribution via the Internet); conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. These individuals often maintain possession of these items for long periods of time.

c. Digital child pornography on a digital device is easy to maintain for long periods of time. Modern digital devices often have extremely large storage capacities. Furthermore, cheap and readily available storage devices, such as thumb drives, external hard drives, and compact discs make it simple for individuals with a sexual interest in children to download child pornography from the Internet and save it – simply and securely – so it can be accessed or viewed indefinitely.

d. Furthermore, even if a person deleted any images of child pornography that may have been possessed or distributed, there is still probable cause to believe that there will be evidence of the illegal activities – that is, the possession, receipt, and/or distribution of child pornography – on the SUBJECT DEVICE. Based on my training and experience, as well as my conversations with digital forensic experts, I know that remnants of such files can be recovered months or years after they have been deleted from a computer device. Evidence that child pornography files were downloaded and viewed can also

be recovered, even after the files themselves have been deleted, using forensic tools. Because remnants of the possession, distribution, and viewing of child pornography is recoverable after long periods of time, searching the SUBJECT DEVICE could lead to evidence of the child exploitation offenses.

V. TRAINING AND EXPERIENCE ON CHILD EXPLOITATION OFFENSES, COMPUTERS, THE INTERNET, AND DEFINITION OF TERMS

11. In this affidavit, the terms "minor," "sexually explicit conduct," "visual depiction," "producing," and "child pornography" are defined as set forth in 18 U.S.C. § 2256. The term "computer" is defined as set forth in 18 U.S.C. § 1030(e)(1).

12. Based upon my training and experience in the investigation of child pornography and information relayed to me by other law enforcement officers involved in the investigation of child pornography, I know the following information about the use of computers with child pornography:

a. Computers and Child Pornography. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. Child pornographers can now produce both still and moving images directly from a common video camera and can convert these images into computer-readable formats. The use of digital technology has enabled child pornographers to electronically receive, distribute, and possess large numbers of child exploitation images and videos with other Internet users worldwide.

b. Computer users can choose their method of storing files: either on a computer's hard drive, an external hard drive, a memory card, a USB thumb drive, a smart phone or other digital media device, etc. (i.e., "locally") or on virtual servers accessible from any digital device with an Internet connection (i.e., "cloud storage"). Computer users frequently transfer files from one location to another, such as from a phone to a computer or from cloud storage to an external hard drive. Computer users also often create "backup," or duplicate, copies of their files. In this way, digital child pornography is extremely mobile and such digital files are easily reproduced and transported. For example, with the click of a button, images and videos containing child pornography can be put onto external hard drives small enough to fit onto a keychain. Just as easily, these files can be copied onto compact disks and/or stored on mobile digital devices, such as smart phones and tablets. Furthermore, even if the actual child pornography files are stored on a "cloud," files stored in this manner can only be accessed via a digital device. Therefore, viewing this child pornography would require a computer, smartphone, tablet, or some other digital device that allows the user to access and view files on the Internet.

c. Internet. The term "Internet" is defined as the worldwide network of computers -- a noncommercial, self-governing network devoted mostly to communication and research with roughly 500 million users worldwide. The Internet is not an online service and has no real central hub. It is a

collection of tens of thousands of computer networks, online services, and single user components. In order to access the Internet, an individual computer user must use an access provider, such as a university, employer, or commercial Internet Service Provider ("ISP"), which operates a host computer with direct access to the Internet.

d. Internet Service Providers. Individuals and businesses obtain access to the Internet through ISPs. ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers; remotely store electronic files on their customer's behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or businesses that have subscriber accounts with them. Those records often include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, and other information both in computer data and written record format.

e. IP Addresses. An Internet Protocol address ("IP Address") is a unique numeric address used to connect to the Internet. An IPv4 IP Address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). In simple terms, one computer in a home may connect directly to the Internet with an IP Address assigned by an ISP. What is now

more typical is that one home may connect to the Internet using multiple digital devices simultaneously, including laptops, tablets, smart phones, smart televisions, and gaming systems, by way of example. Because the home subscriber typically only has one Internet connection and is only assigned one IP Address at a time by their ISP, multiple devices in a home are connected to the Internet via a router or hub. Internet activity from every device attached to the router or hub is utilizing the same external IP Address assigned by the ISP. The router or hub "routes" Internet traffic so that it reaches the proper device. Most ISPs control a range of IP Addresses. The IP Address for a user may be relatively static, meaning it is assigned to the same subscriber for long periods of time, or dynamic, meaning that the IP Address is only assigned for the duration of that online session. Most ISPs maintain records of which subscriber was assigned which IP Address during an online session.

f. IP Address – IPv6. Due to the limited number of available IPv4 IP addresses, a new protocol was established using the hexadecimal system to increase the number of unique IP addresses. An IPv6 consists of eight sets of combination of four numbers 0-9 and/or letters A through F. An example of an IPv6 IP address is 2001:0db8:0000:0000:0000:ff00:0042:8329.

g. The following definitions:

i. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly

and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

ii. "Chat room," as used herein, refers to the ability of individuals to meet in one location on the Internet in order to communicate electronically in real-time to other individuals. Individuals may also have the ability to transmit links to electronic files to other individuals within the chat room.

iii. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

iv. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where: (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

v. "Cloud-based storage," as used herein, is a form of digital data storage in which the digital data is stored on remote servers hosted by a third party (as opposed to, for example, on a user's computer or other local storage device) and is made available to users over a network, typically the Internet. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to a file stored on a cloud-based service does not need to be a user of the service to access the file. Access is typically free and readily available to anyone who has an Internet connection.

vi. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. See 18 U.S.C. § 1030(e)(1).

vii. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data.

Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

viii. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

ix. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which

perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

x. "File Transfer Protocol" ("FTP"), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

xi. "Encryption" is the process of converting data into a code in order to prevent unauthorized access to the data.

xii. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

xiii. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

xiv. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

xv. "Log files" are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

xvi. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

xvii. "Mobile applications," as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

xviii. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

xix. "Remote computing service," as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

xx. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

xxi. A "storage medium" or "storage device" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

xxii. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

xxiii. A "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

13. Because file(s) containing child pornography were found on the SUBJECT DEVICE, there is probable cause to believe that evidence of the Subject Offenses will be found within the SUBJECT DEVICE.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this ___ day of September, 2022.

_____

HONORABLE ALEXANDER F. MACKINNON
UNITED STATES MAGISTRATE JUDGE

EXHIBIT 1

UNITED STATES DISTRICT COURT

for the

Central District of California

FILED
CLERK, U.S. DISTRICT COURT
8/11/2022
CENTRAL DISTRICT OF CALIFORNIA
BY: ib DEPUTY

In the Matter of the Search of

A pink/peach Samsung cellular phone with IMEI 351488824003851 and a blue Motorola cellular phone with IMEI 351488824003851, both seized on August 2, 2022, as described more fully in Attachment A.

Case No. **2:22-MJ-03149**

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A

located in the Central District of California, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is:

☒ evidence of a crime;

☒ contraband, fruits of crime, or other items illegally possessed;

☒ property designed for use, intended for use, or used in committing a crime;

☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. § 841(a)(1), 846	Possession with Intent to Distribute Controlled Substances; Conspiracy

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (*give exact ending date if more than 30 days*: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Sean D. Lusk
Applicant's signature

TFO Sean D. Lusk
Printed Name and Title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: 8/11/2022

Judge's signature

City and state: Los Angeles, CA

Hon. Alexander F. MacKinnon, U.S. Magistrate Judge
Printed Name and Title

AUSA: Kathrynne Seiden (x0631)

ATTACHMENT A

ITEMS TO BE SEARCHED

The following digital devices (the "SUBJECT DEVICES"), seized on August 2, 2022, and currently maintained in the custody of the Federal Bureau of Investigation in Santa Maria, California:

1. A pink/peach Samsung cellular phone with IMEI # 351488824003851.

2. A blue Motorola cellular phone with a cracked screen, seized on August 2, 2022, from the person of Timothy Daniel Espinoza.

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 21 U.S.C. §§ 841(a)(1) (possession with intent to distribute controlled substances) and 846 (conspiracy to distribute controlled substances) (the "Subject Offenses"), namely:

a. Records, documents, programs, applications and materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

b. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email communications or other text or written communications sent to or received from any of the digital devices and which relate to the above-named violations;

c. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device and which relate to the above-named violations;

d. Records, documents, programs, applications, materials, or conversations relating to the trafficking of drugs, including ledgers, pay/owe records, distribution or customer lists, correspondence, receipts, records, and documents noting price, quantities, and/or times when drugs were bought, sold, or otherwise distributed;

e. Audio recordings, pictures, video recordings, or still captured images related to the purchase, sale, transportation, or distribution of drugs;

f. Contents of any calendar or date book;

g. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations; and

h. Any SUBJECT DEVICE which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.

i. With respect to any SUBJECT DEVICE containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as

viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

II. SEARCH PROCEDURE FOR THE SUBJECT DEVICES

3. In searching the SUBJECT DEVICES (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") may search any SUBJECT DEVICE capable of being used to facilitate the above-listed violations or containing data falling within the scope of the items to be seized.

b. The search team will, in its discretion, either search each SUBJECT DEVICE where it is currently located or transport it to an appropriate law enforcement laboratory or similar facility to be searched at that location.

c. The search team shall complete the search of the SUBJECT DEVICES as soon as is practicable but not to exceed 120 days from the date of issuance of the warrant. The government will not search the SUBJECT DEVICES beyond this 120-day period without obtaining an extension of time order from the Court.

d. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each SUBJECT DEVICE capable of containing any of the items to be seized to the search protocols to determine whether the SUBJECT DEVICE and any data thereon falls within the scope of the items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or

encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of the items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

e. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

f. If the search determines that a SUBJECT DEVICE does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the SUBJECT DEVICE and delete or destroy all forensic copies thereof.

g. If the search determines that a SUBJECT DEVICE does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

h. If the search determines that a SUBJECT DEVICE is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital

device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

i. The government may also retain a SUBJECT DEVICE if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

j. After the completion of the search of the SUBJECT DEVICES, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

4. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

5. During the execution of this search warrant, law enforcement is permitted to (1) depress MCLAUGHLIN's and/or ESPINOZA's thumb- and/or fingers onto the fingerprint sensor of the SUBJECT DEVICES (only if the device has such a sensor), and

direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of MCLAUGHLIN's and/or ESPINOZA's face with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

6. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AFFIDAVIT

I, Sean D. Lusk, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of an application for a warrant to search the following digital devices (the "SUBJECT DEVICES"), seized on August 2, 2022 and currently in the custody of the Federal Bureau of Investigation ("FBI") in Santa Maria, California, as described more fully in Attachment A:

a. A pink/peach Samsung cellular phone with IMEI 351488824003851, seized on August 2, 2022 ("SUBJECT DEVICE 1").

b. A blue Motorola cellular phone with a cracked screen, seized on August 2, 2022 from the person of Timothy Daniel Espinoza ("ESPINOZA") ("SUBJECT DEVICE 2").

2. The requested search warrant seeks authorization to seize evidence, fruits, or instrumentalities of violations of 21 U.S.C. §§ 841(a)(1) (possession with intent to distribute controlled substance) and 846 (conspiracy and attempt to distribute controlled substance) (collectively, the "Subject Offenses"), as described more fully in Attachment B. Attachments A and B are incorporated herein by reference.

3. The facts set forth in this affidavit are based upon my personal observations, my training and experience, information obtained from various law enforcement reports, and my review of evidence in this case, including body and patrol vehicle dash camera footage and 911 and California Highway

Patrol ("CHP") Dispatch audio recording. This affidavit is intended to show merely that there is sufficient probable cause for the requested search warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only and all dates are approximate.

II. BACKGROUND OF AFFIANT

4. I am a Task Force Officer ("TFO") with the FBI assigned to the Central Coast Safe Streets Task Force. I am also employed as a full-time, sworn law enforcement officer for the CHP and have been for the past 23 years. I am currently assigned to the Coastal Division Investigative Services Unit. My primary responsibility is to investigate and assist other officers and allied agencies with in-depth investigations involving criminal street gangs, weapons, and narcotics violations.

5. I attended and graduated from the California Highway Patrol Academy and hold Basic, Intermediate, and Advanced Certificates from California Peace Officer Standards and Training. I have completed a 72-hour Drug Recognition Expert course certified by the International Association of Chiefs of Police and over 80 hours of narcotics and criminal interdictions training relating to the transportation, concealment, trends, and sales of illegal narcotics and other criminal activities. I have spoken on numerous occasions with other officers and

experts in the field of narcotics interdiction regarding current trends on narcotic sales and trafficking.

6. As a TFO, I have participated in numerous investigations involving federal firearm and drug offenses and participated in the execution of numerous arrest and search warrants. I have also participated in the interviews of defendants, informants, and witnesses who had personal knowledge of firearm and drug trafficking methods.

III. SUMMARY OF PROBABLE CAUSE

7. On August 2, 2022, Lorianne Kanani McLaughlin ("MCLAUGHLIN") called 911 to report that she was being physically assaulted by her boyfriend in a car. CHP officers found MCLAUGHLIN sitting in the backseat of a car parked near the off-ramp of the U.S. 101 freeway and found MCLAUGHLIN's boyfriend, ESPINOZA, nearby.

8. After interviewing MCLAUGHLIN and ESPINOZA, officers arrested ESPINOZA for domestic violence. As they were doing so, ESPINOZA made spontaneous statements indicating that MCLAUGHLIN was keeping drugs in the car. One of the CHP officers also saw drug paraphernalia sitting in an open toiletry case in the car. A drug detection dog alerted to the possible presence of drugs near the center console. Officers searched the car and found approximately 517.4 grams of methamphetamine.

9. Officers seized SUBJECT DEVICE 1 from the back passenger area, near where MCLAUGHLIN had been sitting. Officers seized SUBJECT DEVICE 2 from ESPINOZA's person.

IV. STATEMENT OF PROBABLE CAUSE

10. Based on my training and experience, my conversations with law enforcements officers, my personal observations, and my review of the law enforcement reports related to and evidence seized during MCLAUGHLIN's and ESPINOZA's arrests, including body and patrol vehicle dash camera footage and 911 and CHP Dispatch audio recordings, I am aware of the following information.

A. CHP Dispatch Relays 911 Calls Related to an SUV

11. On August 2, 2022, around 10:59 a.m., CHP Dispatch broadcasted a "be on the look out" ("BOLO") for an older brown SUV. A caller had reported that the SUV was speeding, an occupant was throwing bottles out the window, and a passenger in the back seat was waving at passing motorists. The reporting party relayed that the vehicle exited the southbound U.S. 101 freeway at Los Alamos and "stopped all crazy."

12. Approximately nine minutes later, at 11:08 a.m., CHP Dispatch told CHP Officer Medina to respond to the Bell Street off-ramp of the U.S. 101 freeway for a possible domestic violence incident that occurred near the Los Alamos exit. An individual later identified as MCLAUGHLIN had called 911 and told the operator that her boyfriend, later identified as ESPINOZA, was physically assaulting her from inside a silver Chevrolet Suburban. Both MCLAUGHLIN and ESPINOZA then called 911 several times to report each other.

13. CHP Dispatch told Officer Medina that the car from the BOLO call might be the same one related to the domestic violence call.

B. CHP Officer Medina Locates MCLAUGHLIN and ESPINOZA

14. At approximately 11:12 a.m., Officer Medina saw a silver Chevrolet Suburban parked on Bell Street and Cat Canyon Road, near the northern Los Alamos exit of the southbound U.S. 101 freeway. MCLAUGHLIN was seated in the rear seating area, which had been converted into a sleeping area, with the door open. Officer Medina spoke with MCLAUGHLIN about the reported incident and asked MCLAUGHLIN whether she needed medical attention, which she declined. At approximately 11:18 a.m., Officer Gruver arrived on scene to assist Officer Medina with interviewing MCLAUGHLIN.

15. Meanwhile, at approximately 11:17 a.m., CHP Officers Larson and Jacobs located ESPINOZA, standing approximately 150 yards south of the Suburban, at the intersection of Bell Street and Cat Canyon Road. Officer Larson saw that ESPINOZA was holding SUBJECT DEVICE 2. Officer Larson searched ESPINOZA for weapons, handcuffed him, and placed his property, including SUBJECT DEVICE 2, into a secure bag. Officer Larson and Officer Jacobs then transported ESPINOZA by car back to Officer Medina, near the Suburban.

16. After ESPINOZA arrived back at Officer Medina's location, officers removed ESPINOZA's handcuffs and Officer Medina interviewed ESPINOZA about the alleged domestic violence incident.

17. Meanwhile, CHP Officer Gruver interviewed MCLAUGHLIN while she was seated in the left rear seat area of the SUBJECT VEHICLE. CHP Officer Jacobs assisted Officer Gruver. According to Officer Jacobs' report, Officer Jacobs could smell the strong odor of unburnt marijuana coming from within the Suburban. Officer Jacobs also saw an open toiletry bag containing a small glass pipe that Officer Jacobs knows to be commonly utilized for smoking narcotics. Officer Jacobs also noted two small glass mirrors with a clear powdery substance on top, near the instrument panel.

18. At approximately 11:58 a.m., Officer Medina arrested ESPINOZA for felony domestic violence.

19. While Officer Medina was handcuffing ESPINOZA, ESPINOZA made a spontaneous statement to Officer Medina and CHP Sergeant Ferguson, referring to MCLAUGHLIN as a "fucking drug dealer." ESPINOZA suggested that the officers were going to let MCLAUGHLIN "get away with all those drugs" in her car. ESPINOZA added that MCLAUGHLIN had "over half a fucking pound in there."

20. After ESPINOZA was arrested, Sergeant Ferguson related ESPINOZA's statement about the drugs to Officer Jacobs. Officer Jacobs directed his drug detection dog, Rudi, to conduct an exterior sniff of the car. Officer Jacobs noted that Rudi had an obvious change of behavior at the passenger door. Officer Jacobs directed Rudi inside the car and Rudi had an immediate "focused indication" towards the center console area, reflecting a positive alert indicating the presence of drugs or items recently contaminated with the odor of drugs in that location.

C. Officers Search the Suburban and Find SUBJECT DEVICE 1 and Suspected Narcotics

21. Officers then searched the Suburban. Underneath the cup holder area in the center console, officers found plastic packaging containing what the officers suspected was methamphetamine. Officers also found additional suspected narcotics, including heroin and marijuana, in the passenger compartment, along with several empty re-sealable plastic bags.

22. During the search of the car, CHP Officer Larson seized SUBJECT DEVICE 1 from the rear seating area, which had been converted into a sleeping area.

23. At approximately 12:46 p.m., Officers arrested MCLAUGHLIN for felony narcotics transportation for the purpose of sales. Officers had the Suburban towed and impounded.

24. Based on records retrieved by CHP, the car is registered to MCLAUGHLIN at an address in Orcutt, California.

25. The SUBJECT DEVICES are currently in the custody of FBI in Santa Maria, California.

D. The Suspected Narcotics Test Presumptively Positive for Methamphetamine

26. On August 8, 2022, I obtained the evidence seized by CHP on August 2, 2022. I observed three plastic packages, including two Ziploc plastic bags and one plastic container containing suspected methamphetamine, weighing 517.4 grams in total. I conducted a field test of the substance from each of the three packages. All three tested presumptively positive for methamphetamine.

27. I processed and sent each of the three packages to the Drug Enforcement Agency Southwest Laboratory for chemical analysis. I processed and placed the remaining items I obtained from CHP, including the SUBJECT DEVICES, into evidence.

V. TRAINING AND EXPERIENCE ON DRUG OFFENSES

28. Based on my training and experience and familiarity with investigations into drug trafficking conducted by other law enforcement agents, I know the following:

a. Drug trafficking is a business that involves numerous co-conspirators, from lower-level dealers to higher-level suppliers, as well as associates to process, package, and deliver the drugs and launder the drug proceeds. Drug traffickers often travel by car, bus, train, or airplane, both domestically and to foreign countries, in connection with their illegal activities in order to meet with co-conspirators, conduct drug transactions, and transport drugs or drug proceeds.

b. Drug traffickers often maintain books, receipts, notes, ledgers, bank records, and other records relating to the manufacture, transportation, ordering, sale and distribution of illegal drugs. The aforementioned records are often maintained where the drug trafficker has ready access to them, such as on their cell phones and other digital devices.

c. Communications between people buying and selling drugs take place by telephone calls and messages, such as e-mail, text messages, and social media messaging applications, sent to and from cell phones and other digital devices. This includes sending photos or videos of the drugs between the

seller and the buyer, the negotiation of price, and discussion of whether or not participants will bring weapons to a deal. In addition, it is common for people engaged in drug trafficking to have photos and videos on their cell phones of drugs they or others working with them possess, as they frequently send these photos to each other and others to boast about the drugs or facilitate drug sales.

d. Drug traffickers often keep the names, addresses, and telephone numbers of their drug trafficking associates on their digital devices. Drug traffickers often keep records of meetings with associates, customers, and suppliers on their digital devices, including in the form of calendar entries and location data.

e. Individuals engaged in the illegal purchase or sale of drugs and other contraband often use multiple digital devices.

VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

29. As used herein, the term "digital device" includes the SUBJECT DEVICES.

30. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained

in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

31. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

32. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress MCLAUGHLIN's and/or ESPINOZA's thumb

and/or fingers on the device(s); and (2) hold the device(s) in front of MCLAUGHLIN's and/or ESPINOZA's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

33. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VII. CONCLUSION

34. For the reasons described above, there is probable cause that the items to be seized described in Attachment B will be found in within the SUBJECT DEVICES, as described in Attachment A.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 11th day of August, 2022.

HONORABLE ALEXANDER F. MACKINNON
UNITED STATES MAGISTRATE JUDGE